

Subject

State Telecommunication Network, Acceptable Use

For

EMPLOYEE HANDBOOK
All Users of State Telecommunication
Network

Also See

ET-03094, 102, 116

Identification	5/112-5/115 ET-03141 Policy
Effective	3-1-2000
Through	3-1-2002
	Page 1 of 4
Replaces	New

Page 5/112

All users of state networks must comply with the state's acceptable use policy.

The purpose of the state telecommunication network is to facilitate information exchange in support of state government functions. These resources and value-added services are primarily intended to assist state employees in the performance of their assigned state Government tasks. The state reserves the right to monitor and log all network activity, including e-mail, with or without notice, and therefore users should have no expectation of privacy in the use of these resources.

Use of the state telecommunication infrastructure is a revocable privilege, requiring compliance and conformity with this acceptable use policy. Agencies must enforce this policy and inform their employees and contractors of this policy. Contractors, who need and are granted access by the agency to the state network, are restricted to only those resources necessary to accomplish their contractual, legal or administratively assigned state government task.

The following restates the information in Procedure 1310.16, issued January 6, 1997, by the Department of Management and Budget (DMB), Automation Services Division.

State Network Users' Responsibilities

- Make a reasonable effort to inform themselves of and comply with the acceptable use policies of each system and external network they intend to access, prior to their attempting access.
- Respect the privacy and ownership privileges of other users. Unless authorized to do so, users shall not intentionally seek information on, obtain copies of, use, modify, or place on openly accessible information servers, files and other data which are exempt or excluded from public disclosure pursuant to the Freedom of Information Act (FOIA), PA 442 of 1976, as amended. Release, distribution and handling of FOIA documents and data must conform with Administrative Procedure 2410.01, issued January 1, 1994 and applicable department procedures regarding denial of FOIA requests and other state and federal laws.
- Respect the legal protection provided by copyright and license to programs and data. No software copy is to be made by any user without a prior, good faith determination that such copying is, in fact, permissible and that the licensing restrictions have been met.

Initials

Signature

Page 5/113

- Respect the integrity of passwords and/or authentication pass phrases by complying with state security policy. The exchanging of passwords or seeking the password of others is explicitly prohibited.
- Respect the integrity of computing systems by not intentionally taking actions or developing programs that either harass other users or obstruct a computer system. Users shall not damage, alter, or disrupt computers or maliciously use computer systems whose usage is protected by law, regulation, or administrative policy.
- Respect the integrity of connected computer systems by insuring that imported files are virus free.
- Not represent themselves electronically as others, either on state networks or elsewhere, unless explicitly authorized to do so by those other users. Users must not circumvent established, system-specific policies defining eligibility for resource access.
- Be good network citizens by being cognizant of and conservative in the bandwidth demands their applications (especially those using video or image transmissions) make on the network. Future bandwidth contention may necessitate restrictions.

Acceptable Uses of the Telecommunication Network

- Communication and exchange directly relating to the mission, charter and work tasks of the state agency.
- Announcements of new state laws, procedures, policies, services or activities, but not commercial advertising.
- Use for advisory, standards, research, analysis and professional society activities related to the user's state governmental duties.
- Use in applying for or administering grants or contracts for state government research or programs, but not for non-state-government-related fund-raising or public relations activities.
- Communication and exchange for professional development, to maintain currency, or debate issues related to that user's assigned state governmental activities.

Prohibited Uses of the Telecommunication Network

- Use which is illegal.
- Use which violates the security, privacy and confidentiality policies, practices and laws of the state and release of material which is exempt from disclosure as listed in section 13 of the Freedom of Information Act (Public Act 442 of 1976 as amended).
- Use for access to, display of or distribution of: (a) indecent or obscene material (re US Supreme Court Miller v California 1973 and Ginsberg v New York 1968), (b) child pornography (re 18 US Code 2252), or (c) material in violation of Civil Service Rule 1-2.2 or departmental regulations prohibiting sexual harassment.
- Use for profit activities unless specific to the charter, mission and duties of the government agency.
- Use for private or personal business transactions, or for partisan or non-partisan political activities.
- Use for playing of games or non-business computer activities which generate traffic or consume bandwidth on any state network segment.

Agency Responsibilities

- Agency Chief Information Officers or their delegated representative are responsible for compliance with provisions of this procedure and for investigating suspected non-compliance. These duties include the following:
 - Investigation of alleged or suspected non-compliance with the provisions of this policy. These are to be conducted with due regard for the privacy rights of all persons and users involved.
 - Suspension of service to users when deemed necessary for the operation and/or integrity of the state communication infrastructure or connected networks. Use privileges, user accounts and/or password access may be withdrawn without notice.
 - When an instance of non-compliance is suspected or discovered in a computing system or network connected to the state network, the agency shall proceed in accordance with departmental and Civil Service rules. Internal discipline, up to and including discharge, may be appropriate in some cases of non-compliance with this policy. Criminal or Civil action may be initiated in appropriate instances.

Subject

State Telecommunication Network, Acceptable Use

Identification

5/112-5/115

ET-03141

Policy

Effective

3-1-2000

Through

3-1-2002

Page 4 of 4

*Page 5/115***DMB Office of Information Technology Responsibilities**

- Maintain this procedure to be in conformance with relevant administrative directives, Michigan Laws and advances in technology.
- Disseminate changes in procedure to all departments and agencies as needed, but no less than annually.

End